

IN THE CLAIMS:

Please cancel claims 1-37 and substitute new claims 38-47 as follows:

1.-37. (CANCEL)

38. (NEW) A method of protecting a device against unintended use in a secure environment, the device being adapted to execute applications that involve conditional access to at least one of valuable contents and services, and the device including an integrated circuit that has a central processing unit, an internal memory and input/output connections for external memory incorporated on a single chip, comprising the steps of:

encrypting sensitive application code and data with a secret key stored in a secured memory area of the internal memory for uniquely linking said external memory and said chip, the encrypted code and data being then stored in said external memory; and

encrypting a random number and a hash value of the random number with said secret key, the encrypted random number and hash value being decrypted with the secret key at least on each reset of the device, and

allowing decryption of the encrypted sensitive code and data only if the decrypted hash value equals a hash value calculated from the decrypted random number.

39. (NEW) The method of claim 38, wherein the application code is downloaded into the device, encrypted with the secret key and stored in the external memory.

40. (NEW) A method of protecting a device against unintended use in a secure environment, the device being adapted to execute applications that involve secure

transactions and/or conditional access to valuable contents and/or services, and the device including an integrated circuit that has a central processing unit, an internal memory and input/output connections for external memory incorporated on a single chip, comprising the steps of:

- a) signing any application code down-loaded into the device with a private key of an asymmetric key pair and proper execution of the application is subject to a verification of the signature with a public key of said key pair;
- b) encrypting sensitive application code and data with a secret key stored in a secured memory area of the internal memory for uniquely linking said external memory and said chip, and storing the encrypted code and data in an external memory;
- c) encrypting a random number and a hash value of the random number with said secret key and storing the encrypted random number and hash value in the external memory;
- d) on each reset of the device, decrypting the encrypted random number and hash value with the secret key; and
- e) allowing decryption of the encrypted sensitive code and data only if the decrypted hash value equals a hash value calculated from the decrypted random number.

41. (NEW) The method of claim 38, wherein, after manufacturing of the chip and prior to delivery to a customer, a secret access channel is established to write a secret personalization key into the secure memory area.

42. (NEW) The method of claim 41, wherein the content of the secure memory area is protected by calculating a hash value of the secure memory area content and writing the hash value into the secure memory area.

43. (NEW) The method of claim 41, wherein a personalization application is signed with a Secure Architecture Designer's private key and then encrypted with the secret personalization key, the personalization application is loaded into the device and decrypted with the secret personalization key, the signature of the personalization application is checked with the Secure Architecture Designer's public key, and the personalization application is executed to write sensitive personalization data into the secure memory area.

44. (NEW) The method of claim 41, wherein a personalization application is encrypted with a secret symmetric key stored in a secured memory area of the device, a hash value of the personalization application is signed with a Secure Architecture Designer's private key, the encrypted personalization application and the signed hash value are loaded into the device, the personalization application is decrypted with the secret symmetric key, the signature of the hash value is checked with the Secure Architecture Designer's public key stored in the read only memory of the device, and the personalization application is executed to write sensitive personalization data into the secure memory area.

45. (NEW) The method of claim 41, wherein a personalization application and a hash value of the personalization application signed with a Secure Architecture Designer's private key are encrypted with a secret symmetric key stored in a secured memory area of the device, the encrypted personalization application and signed hash value are loaded into the device, the personalization application and signed hash value are decrypted with the secret

symmetric key, the signature of the hash value is checked with the Secure Architecture Designer's public key stored in the read only memory of the device, and the personalization application is executed to write sensitive personalization data into the secure memory area.

46. (NEW)        The method of claim 38, wherein the external memory includes a RAM and the chip has a bi-directional encryption/decryption hardware interface ensuring high performance and already encrypted exchange of data between the chip and the RAM.

47. (NEW)        The method according to claim 38, wherein said chip is provided with a random number generator and a hash value is obtained from a random number generated by the random number generator, the random number with its hash value are encrypted with said secret key, and the encrypted random number with its hash value are stored in the external memory.